Study of Various Methods for Securing Data Communication

Shubhra Goel[1] Seema Mehla[2]
[1, 2]Doon Valley Institute of Engg. & Tech Karnal, India

Abstract---In this modern era, with a lot of internet based applications various organizations, companies, govt. agencies, etc. communicate digitally. A lot of multimedia data are generated and transmitted which are easier to edit, modify and duplicate. So sharing this data is a critical issue due to security problems. Hence some techniques are needed to protect the shared data. Cryptography is a technique by which the original data can be converted to some other format by the help of a key which without the knowledge of key cannot be read by an outsider. We can make this communication more secure by using the concept of Steganography along with Cryptography. Steganography is hiding the sensitive information in some media e.g. hiding a text file in an image file, etc. to transfer the information securely over the communication network. This paper presents various encryption and steganography techniques that are in practice today.

Keywords: Steganography, Cryptography, Encryption, DES, TDES, Blowfish, RSA, AES, LSB.

I. Introduction

Data security is an essential part of an organization; it can be achieved by using various methods. Computers are interconnected with each other in the multi node network and therefore are exposed to various networks and communication channels so data security is a critical issue.

Here encryption is required to keep the data confidential from each other. Only the authorized person should have the capability to read the message. Data cryptography mainly is the scrambling of the content of data, such as text, image, audio, video, etc. Encryption is done using a key and security. Original message is called plain text and after its encryption it is called cipher text[1]. There are two main techniques for encryption – substitution and permutation. Substitution is mapping if one value to another and permutation is reordering of bit positions for each of the inputs. These techniques are used a number of times in iterations called rounds.

Cryptography involves 4 steps:

Step. 1 : Selection of the original text to be encrypted.
Step. 2 : Applying a function or algorithm for encryption/decryption.
Step. 3 : Distribution of message bits in blocks of data according to algorithm used.
Step. 4 : Use a key as required by the selected algorithm.
Step. 5 : Giving the plain text and key as parameters to the algorithm or function.

Steganography is a technique which hides the existence of the message itself by hiding the message in some other file for e.g. if a confidential text file is hidden in an image file like of a bird, cartoon, etc. the intruder will see some random image transferring through the network and will not be able to figure out any confidential data transfer. Nearly all digital file formats can be used for steganography. Steganography in which image file is used as a cover file is called image steganography.

Steganography involves 4 steps:

(1) Selection of the cover media in which the data will be hidden.
(2) The secret message or information that is needed to be hidden in the cover image.
(3) A function that will be used to hide the data in the cover media and its inverse to retrieve the hidden data.
(4) An optional key or password to authenticate or to hide and unhide the data.

The rest of the paper is organized as follows: Section II and Section III discuss types of cryptographic algorithms and image steganography respectively. Comparison and contrast of steganography and cryptography is shown in Section IV. Section V and Section VI discusses various encryption algorithms and image steganography techniques respectively. The paper ends with the conclusion in Section VII.

II. Types of Cryptographic Algorithms

Cryptography can be classified as:

a) *Symmetric Key Cryptography*- In this, same key is used at the sender and receiver side i.e. for encryption and decryption resp. It is also known as private key cryptography or secret key cryptography. This key is also to be distributed between the two parties. There are various symmetric key algorithms such as DES, TDES, AES, RSA, Blowfish[2].
b) *Asymmetric Key Cryptography*- In this, different keys are used for encryption and decryption – public and private key. It is also known as public key cryptography. The public key of the receiver is used to encrypt the message and only the private key of the receiver can be used to decrypt the cipher text[1].
c) *Hash Functions*- They are also called message digests. These algorithms do not use a key; instead, a fixed-length hash value is computed based upon the plain text that makes it impossible to recover the plain text by an outsider.

III. Types of Image Steganography

Image Steganography is divided into following categories:

a) *Spatial Domain Steganography*- It is also known as substitution technique. In this the message is inserted in the pixels of the image by employing different methods
b) *Transform Domain Steganography*- It is also known as frequency domain technique. Here pixel values are transformed and then processing is applied on the transformed coefficients. This technique hides information in the areas of the image that is less exposed to compression, cropping and image processing.

c) *Spread Spectrum Steganography*- When employed with steganography, spread spectrum either deals with the cover image as noise or tries to add pseudo-noise to the cover image. In pseudo-noise technique, the hidden data is spread throughout the cover image and so it becomes difficult to detect[15].

d) *Statistical Methods*- These techniques tend to modify the statistical properties of an image in addition to preserve them in the embedding process. The modification done is typically small[15].

IV. STEGANOGRAPHY VERSES CRYPTOGRAPHY

Steganography and cryptography algorithms share some common and contrasting features. The following table shows comparison and contrast between steganography and cryptography.

S. No.	**Context**	**Steganography**	**Cryptography**
1	Host Files	Image, Audio, Text, etc.	Mostly Text Files
2	Hidden Files	Image, Audio, Text, etc.	Mostly Text Files
3	Result	Stego File	Cipher Text
4	Type of Attacks	Staganalysis: Analysis of a file with an objective of finding whether it is stego file or not.	Cryptanalysis

Table. 1: Steganography Vs Cryptography

V. VARIOUS ENCRYPTION ALGORITHMS

In this section, various encryption algorithms that will facilitate secure data transmission over the underlying communication network are discussed. These algorithms are block cipher which means that they can encrypt/decrypt multiple bits of data at a time. The number of bits depends upon the algorithm used.

A. Data Encryption Standard (DES)

DES is a symmetric, 64 bit block cipher as it uses same key for encryption and decryption, and it operates on 64 bit blocks of data at a time. There are 16 rounds in DES. 2 inputs are given to the DES algorithm – plain text to be encrypted and the secret key. Once a plain text message is received to be encrypted, it is arranged into 64 bit blocks required for input. If the number of bits in the message is not evenly divisible by 64, then the last block will be padded. DES accepts a 64 bit key as input, but actual key size is 56 bits out of those 64 bits and the remaining 8 bits are used for parity checking and have no effect on DES's security.

B. Simplified DES (S-DES)

The S-DES encryption algorithm takes an 8-bit block of plaintext and a 10-bit key as input and produces an 8-bit block of cipher text as output. The S-DES decryption algorithm takes an 8-bit block of cipher text and the same 10-bit key used to produce that cipher text as input and produces the original 8-bit block of plaintext[14].

C. Triple DES (TDES)

It was developed to address the flaws in DES without designing a new cryptosystem from scratch. The encryption method is similar to that of DES but applied 3 times to increase the encryption level[3]. It is shown in the figure 1. Therefore, it is termed Triple DES. It takes three 64-bit keys for an overall key length of 192 bits (64*3)[5]. The security of TDES is effective but the main limitation is that it is too time consuming.

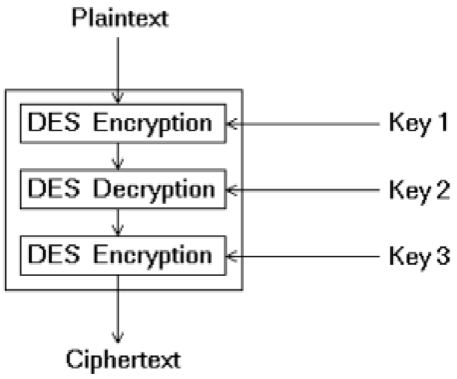

Fig. 1: Implementation of TDES

As shown in the fig. 1, data is encrypted with the first key, decrypted with the second key and finally encrypted again with the third key[5]

D. RSA

RSA is a public key cryptography algorithm[13]. It uses prime numbers to generate public and private key. It uses the block size data in which plain text and cipher text are integers between 0 and n-1 for n values. Size of n is considered 1024 bits or 309 decimal bits[5]. It is widely used for secure communication channel but it is too slow for encrypting large volumes of data.

E. Advanced Encryption Standard (AES)

AES is a symmetric key encryption algorithm. It was developed for the replacement of DES. It uses variable key length of 128, 192 and 256 bits and also there are three different default rounds for these three key length sizes – 10 for 128 bit key size, 12 for 192 bit key size and 14 for 256 bit key size. It can be implemented on various platforms especially in small devices. To provide security AES uses various types of transformations and also it takes many years to test all the possible keys for the weakest version, AES-128[12].

F. Blowfish

Blowfish is also a symmetric key encryption algorithm. It is a 64 bit block cipher and have variable length key from 32 bits to 448 bits. It uses the concept of sub keys generated by the algorithm itself. It is fast, compact, simple and secure[6]. One of the drawbacks of blowfish is that it could be a bit time consuming in some implementations because of its complicated encryption functions.

VI. VARIOUS IMAGE STEGANOGRAPHY TECHNIQUES

In this section, a survey on various data hiding techniques in steganography is given to facilitate secure data transmission over the underlying communication network.

A. Least Significant Bit (LSB)

LSB is a well-known, simple approach in the data hiding field to embed information in a cover image. This method embeds the fixed-length secret bits in the same fixed-length LSBs of pixels. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel.

For example, a grid for 3 pixels of a 24-bit image can be as follows:

(11010011 00101101 00011100)

(10100110 00001101 10011101)

(00101100 10101010 10001101)

When the number 250, whose binary representation is 11111010, is embedded into the LSB of this part of the image, the resulting grid is as follows:

(1101001**1** 0010110**1** 0001110**1**)

(1010011**1** 0000110**1** 1001110**0**)

(0010110**1** 1010101**0** 10001101)

We can see that only the 4 underlined bits needed to be changed to embed the number 250. These changes are very small which cannot be perceived by the human eye so the number 250 or the message is successfully hidden.

B. Hiding Gray Images Using Blocks Method

As vast channels for communication such as the internet are becoming popular, the security of digital media becomes a great concern. The hiding of a message will reduce the probability of detecting this message. This method hides a gray image in one another. The cover is divided into blocks of equal sizes. Each block size equals the size of the embedding image[10].

C. Hiding Secret Message in Edges of the Images Method

Edge based steganography is in which only the sharper edge regions are used for hiding the message while keeping the other smoother regions as they are. It is more difficult to observe changes at the sharper edges than those in smoother regions. In this method Enhanced LSB algorithm is used which can reduce the rate of pixel modification thereby increasing the security both visually and statistically[10].

D. Grey Level Modification Steganography Method

This Steganography method is based on image layers. This method divides the host image into blocks and embeds the corresponding secret message bits into each block using the layers which are made by the binary representation of pixel values. It then performs a search on the rows and columns of the layers for finding the most similar row or column. The location of row/column and its differences from the secret message is then marked by modifying minimum number of bits in the least significant bits of the blocks[10].

E. Optimal Pixel Adjustment Procedure (OPAP)

In this method the pixel value is adjusted after the hiding of the secret data is done to improve the quality of the stego image without disturbing the data hidden. The basic concept of the OPAP is based on the technique proposed in [7].

F. Bit Plane Splicing Technique

An image in which a pixel is represented by 8 bits can be split into 8 layers such that each layer is considered to be a separate image. In this technique, each plane contributes to build the overall image and as we go towards the LSB plane, the information contained decreases. Most of the data is contained in plane 8 and has a major contribution in building the original image[8].

G. Pixel Value Differencing (PVD)

In this method the number of insertion bits is dependent on whether the pixel is an edge area or smooth area. Two methods have been proposed to implement PVD method. First method hides the data in the target pixel by finding the characteristics of four pixels surrounding it. Another method hides the data in the difference between two adjacent pixel values[9].

VII. CONCLUSION

In this paper, discussion is done about cryptography and steganography and some notable differences between both and also various cryptography algorithms and data hiding techniques in steganography are discussed.

ACKNOWLEDGMENT

Thanks to all the authors who are listed below in the list of references.

REFERENCES

[1] Anjali Patil, Rajeshwari Goudar, “A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices”, International Journal of Scientific & Technology Research Vol. 2, Issue 8, August 2013.

[2] Diaa Salama, Abdul. Elminaam, Hatem Mohamed, Abdul Kader and Mohie Mohamed Hadhoud, ―Performance Evaluation of Symmetric Encryption Algorithms‖, International Journal of Computer Science and Network Security, vol.8 No.12, December 2008.

[3] Amritpal Singh, Mohit Marwaha, Baljinder Singh, Sandeep Singh, “Comparative Study of DES, 3DES, AES and RSA”, ISSN 22773061.

[4] Piper,F “Encryption”. Security and Detection, Ecos 97. European Conference.

[5] Megha Zopade, Pragya Shukla, “Analysis of Triple DES and RSA Algorithm in securing Image Steganography”, International Journal of Computer Architecture and Mobility (ISSN 2319-9229), Volume 1-Issue 8, June 2013.

[6] Er. Rajender Singh, Er. Rahul Misra, Er. Vikas Kumar, “Analysis the impact of symmetric cryptographic algorithms on power consumption for various data types”, Interntaional Journal on Recent and innovation Trends in computing and Communication, ISSN 2321-8169, Vol. 1, Issue 4.

[7] Chi-Kwong Chan, L.M. Cheng, Improved hiding data in images by optimal moderately signi7cant-bit replacement, IEE Electron. Lett. 37 (16) (2001) 1017–1018.

[8] M. Naseem, Ibrahim M. hussain, M. Kamran Khan, Aisha Ajmal, “An optimum Modified Bit Plane splicing LSB Algorithm for Secret Data Hiding”, International journal of Computer applications (0975-8887), Vol. 29- No. 12, September 2011.

[9] R. Amirtharajan, R. Akila, P. Deepikachowdavarapu, “A comparative Analysis of Image Steganography”, International journal of Computer applications (0975-8887), Vol. 2- No. 3, May 2010.

[10] Kanzariya Nitin K., Nimavat Ashish V., “Comparison of Various Images Steganography Techniques”, International Journal of Computer Science and Management Research (ISSN 2278-733X), Vol 2 Issue 1, January 2013.

[11] Ali Makhmali, Hajar Mat Jani, “ Comparative study On Encryption Algorithms And Proposing A Data Management Structure”, International Journal of Scientific & Technology Research Vol. 2, Issue 6, June 2013.

[12] Hamdan. O. Alanazi, B.B. Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, “New Comparative Study Between DES, 3DES and AES within Nine Factors”, Journal of Computing, Vol. 2, Issue 3, March 2010, ISSN 2151-9617.

[13] R.Rivest, A. Shamir, L.Adleman. "A method for obtaining digital signatures and public-key cryptosystems"z. Communications of the ACM, Feb 1978.

[14] Ankita agarwal, “ Security Enhancement Scheme for Image Steganography using S-DES Technique”, International Journal of Advanced Research in Computer Science and Software Engineering”, ISSN: 2277 128X, Volume 2, Issue 4, April 2012.

[15] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qershi, “Image Steganography Techniques: An Overview”, International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012